PROTECTION METHOD FOR EMBEDDED SOFTWARE

ABSTRACT OF THE DISCLOSURE

A method for protecting embedded software is proposed which uses a transfer

5   function of the firmware in an electronic information appliance to prevent the execution

of the embedded software in an unauthorized hardware. Before parameters are called

upon, the main program of the embedded software stores the parameters in a buffer.

And through the transfer function, the parameters in the buffer are then shifted

according to a different sequence to another storage interface. As the auxiliary

10 program is subsequently called upon, it does not carry any parameters, since the

parameters are stored in another storage interface. So, the parameters need to be

extracted from a default parameter address and decoded. Correct parameter data is

required to effect a normal execution of the selected function of the software. If the

extracted parameter data is erroneous, execution of embedded software in the

15 unauthorized hardware is disabled.